Quantum secure direct communication network with Einstein-Podolsky-Rosen pairs

Fu-Guo Deng,[1,2,3*] Xi-Han Li,[1,2] Chun-Yan Li,[1,2] Ping Zhou,[1,2] and Hong-Yu Zhou[1,2,3]
[1] *The Key Laboratory of Beam Technology and Material Modification of Ministry of Education,
Beijing Normal University, Beijing 100875, People's Republic of China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering,
Beijing Normal University, Beijing 100875, People's Republic of China*
[3] *Beijing Radiation Center, Beijing 100875, People's Republic of China*

(Dated: February 1, 2008)

We discuss the four requirements for a real point-to-point quantum secure direct communication (QSDC) first, and then present two efficient QSDC network schemes with an N ordered Einstein-Podolsky-Rosen pairs. Any one of the authorized users can communicate another one on the network securely and directly.

PACS numbers: 03.67.Hk, 03.67.Dd, 03.65.Ud

I. INTRODUCTION

The combination of the features of quantum systems with information has produced many interesting and important developments in the field of the transmission and the processing of information. Quantum key distribution (QKD), an important application of quantum mechanics supplies a secure way for creating a private key between two remote parties, the sender, Bob and the receiver, Carol. The noncloning theorem [1] forbids a vicious eavesdropper, Eve to copy perfectly the quantum signal transmitted through the quantum line, and her action will inevitably disturb the quantum system and leave a trick in the results. Bob and Carol can find out Eve by comparing some of the results chosen randomly and analyzing its error rate. Combined with a private key, secret message can be transmitted securely with one-time-pad crypto-system. QKD has progressed quickly [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12] since Bennett and Brassard proposed the standard BB84 QKD protocol [2] in 1984. The reason may be that the modern technology allows QKD to be demonstrated in laboratory [6] and practical applications can be achieved in the future.

Recently, a novel branch of quantum communication, quantum secure direct communication (QSDC) was proposed and actively pursued by some groups [13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26]. With QSDC Bob and Carol can exchange the secret message directly without generating a private key in advance and then encrypting the message, which is different to QKD. In 2002, Beige et al. [26] presented a QSDC protocol in which the message can be read out after the transmission of an additional classical information for each qubit [13, 14, 20], similar to a QKD scheme as each bit of key can represent one bit of secret message with an additional classical information, i.e., retaining or flipping the bit value in the key according to the secret message [13]. The same case takes place in Refs. [17, 18, 19]. In 2002, Boström and Felbinger proposed a ping-pong QSDC following some ideas in quantum dense coding [27] with an Einstein-Podolsky-Rosen (EPR) pair. The authors have claimed that it is secure for generating a private key and quasi-secure for direct communication as it will leak some of the secret message in a noise channel [20]. Wǒjcik and Zhang et al. pointed out that the ping-pong protocol is insecure for direct communication if there are losses in a practical quantum channel [28, 29]. Also, the ping-pong protocol [20] can be attacked without eavesdropping [30, 31]. Cai and Li [21] modified the ping-pong protocol for transmitting the secret message directly by replacing the entangled photons with a single photon in a mixed state, similar to the Bennett 1992 QKD [5]. Meanwhile, Deng et al. put forward a two-step QSDC protocol [13] with EPR pairs transmitted in block and another one based on a sequence of polarized single photons [14]. Wang et al. [15] introduced a QSDC protocol with high-dimension quantum superdense coding. The good nature of the QSDC schemes [13, 14, 15, 16] with quantum data block is that the parties can perform quantum privacy amplification [32, 33, 34] on the unknown states for improving their security in a noise channel. In Ref. [24], Cai and Li designed a protocol for improving the capacity of the ping-pong QSDC protocol [20] with the same way for eavesdropping check as that in Ref. [13]. However, it is not unconditionally secure as the analysis of eavesdropping check depends on the feature of statistics for which a lot of samples should be chosen randomly and measured. Recently, Lucamarini et al. [25] introduced a QSDC protocol for both direct communication and creating a private key with the same ideas in the Refs. [9, 14]. It is secure for QKD, same as Ref. [9], but it is just quasi-secure for direct communication, similar to the QSDC protocol in Ref. [24].

By far, there are many QKD network schemes [35, 36, 37, 38, 39, 40] in which one user can communicate any other one on the network, but not a QSDC network scheme even though there are some point-to-point QSDC schemes [13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26] existing. Moreover, almost all of the existing QSDC point-to-point schemes cannot be used directly to accom-

[*] E-mail addresses: fgdeng@bnu.edu.cn

plish the task in a QSDC network as a distrustful server can steal some information without being detected. In this paper, we will introduce two QSDC network schemes with an ordered N EPR photon pairs. One authorized user can communicate any one on the network securely with the capability of single-photon measurements in the first scheme. As almost all the instances are useful and each EPR photon pair can carry two bits of information, the intrinsic efficiency for qubits and the source capacity are both high. In the second scheme, the users can exploit entanglement swapping to transmit the secret message securely after they set up the quantum channel, the EPR pairs shared. As the qubits encoded by the sender do not suffer from the noise of the quantum line again, its security may be higher than the first one. On the other hand, it has only half the source capacity of the first scheme. Also, the four requirements for a real secure point-to-point quantum direct communication scheme are discussed in detail.

II. THE REQUIREMENTS FOR A REAL QSDC

From the way for transmitting the quantum data and analyzing the security of the quantum channel, all existing QSDC schemes can attributed to one of the two types, the one in which the quantum signal is transmitted in a stream (stream-QSDC) and the other in a quantum data block (QDB-QSDC). The feature of stream-QSDC [20, 21, 22, 23, 24, 25] is that Bob and Carol choose randomly the eavesdropping check mode or the message-coding mode with two asymmetric probabilities for the quantum signal transmitted in a stream (one photon in each round). In the check mode, Bob and Carol obtain a sample for eavesdropping check by means that they choose one or two sets of measuring bases (MBs) to measure it [20, 21, 22, 23, 24, 25]. When they choose the message mode, they encode the secret message on the quantum state directly. In a word, the security check and the encoding of the secret message are done concurrently in stream-QSDC protocols [20, 21, 22, 23, 24, 25]. The property of QDB-QSDC [13, 14, 15, 16, 17, 18, 19] is that the quantum signal is transmitted in a quantum data block. That is, Bob and Carol have to transmit a sequence of quantum states and check its security before Bob encodes the secret message on them. In brief, the encoding of the secret messages is done only after the confirmation of the security of the quantum channel [13, 14, 15, 16] is accomplished.

In essence, the security of quantum communication bases on the two principles: (1). one is the properties of quantum states, such as the uncertainty principle (no-cloning theorem), quantum correlations, nonlocality, and so on; (2). the other is the analysis for quantum error rate based on the theories in statistics. The first principle ensures that Eve cannot copy the quantum states freely as her action will inevitably perturb the quantum systems, which will introduce some errors in the results. The second one is used to check the security of the quantum channel after Bob and Carol transmit the sufficient quantum states. The check for eavesdropping is valid only when Bob and Carol can sample sufficiently enough instances from results transmitted. That is, the message may be secure only when they are obtained after checking eavesdropping.

For QKD Bob and Carol can choose randomly one of two MBs for the quantum states transmitted in one by one as the analysis of the eavesdropping check is just a postprocessing. The security of QKD requires them to determine whether there is an eavesdropper monitoring the quantum channel. The case in QSDC is different to QKD as the two parties cannot abandon the secret message transmitted. In brief, a real point-to-point QSDC protocol should satisfy the four requirements: (1) the secret message can be read out by the receiver directly after the quantum states are transmitted through a quantum channel, and there is no additional classical information exchanged by the sender and the receiver in principle except for those for checking eavesdropping and estimating the error rate. (2) the eavesdropper, Eve cannot obtain an useful information about the secret message no matter what she does; In another word, she can only get a random result for the message with her eavesdropping on the quantum signal. (3) the two legitimate users can detect Eve before they encode the secret message on the quantum states. (4) the quantum states are transmitted in a quantum data block. The last one is not necessary for QKD as the two authorized users just distribute a key which does not include the information about the secret message in this time and can be abandoned if they find out Eve monitoring the quantum channel. QSDC is used for directly communicating the secret message which cannot be discarded. The security of quantum communication depends on the analysis for quantum error rate based on the theories of statistics in which many samples are chosen randomly for its accuracy. In this way, the quantum states should be transmitted in a quantum data block in a QSDC.

From the view of security, the QDB-QSDC protocols [13, 14, 15, 16] are secure with some other quantum techniques, such as quantum privacy amplification [33, 34], in a noise quantum channel. The stream-QSDC protocols [20, 21, 24] are just quasi-secure as the authorized users cannot take a quantum privacy amplification on the quantum states transmitted one by one, which is in principle different to the QDB-QSDC protocols.

III. QSDC NETWORK WITH EPR PAIRS

A. Bidirectional QSDC network

An EPR pair can be in one of the four Bell states [42],

$$|\psi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C - |1\rangle_B|0\rangle_C) \qquad (1)$$

$$|\psi^+\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C + |1\rangle_B|0\rangle_C) \quad (2)$$

$$|\phi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C - |1\rangle_B|1\rangle_C) \quad (3)$$

$$|\phi^+\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|0\rangle_C + |1\rangle_B|1\rangle_C) \quad (4)$$

where $|0\rangle$ and $|1\rangle$ are the eigenvectors of the Pauli operator σ_z (for example the polarizations along the z direction). The subscripts B and C indicate the two correlated photons in each EPR pair. The four local unitary operations U_i ($i = 0, 1, 2, 3$) can transform one of the Bell states into another,

$$U_0 \equiv I = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad (5)$$

$$U_1 \equiv \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \quad (6)$$

$$U_2 \equiv \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (7)$$

$$U_3 \equiv i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \quad (8)$$

where I is the 2×2 identity matrix and σ_i are the Pauli matrices. For example,

$$I \otimes U_0|\psi^-\rangle = |\psi^-\rangle, \qquad I \otimes U_1|\psi^-\rangle = |\psi^+\rangle, \quad (9)$$

$$I \otimes U_2|\psi^-\rangle = |\phi^-\rangle, \qquad I \otimes U_3|\psi^-\rangle = |\phi^+\rangle. \quad (10)$$

Although the topological structure of a QSDC network can be loop or star, similar to QKD network [35, 36, 37, 38, 39, 40], its subsystem can be simplified to that in Fig.1. That is, a QSDC network is composed of many subsystems (the small network cells) and there are three roles in each cell, the server (Alice), the sender (Bob) and the receiver (Carol). Alice provides the service for preparing the quantum signal. Bob is the man who wants to send a message to Carol privately. If Bob and Carol are not in the same branch on the network [38], we assume that the server of the branch with the sender Bob provides the service for preparing the quantum signal, and the other servers provide the quantum line for Bob and Carol (forbid all the others to use it) in a time slot [39]. Then the principle of this QSDC network is explicit if we describe clearly the subsystem in Fig.1.

Now, let us describe our bidirectional QSDC network scheme in detail. First, we only consider the ideal condition. That is, we assume that there is no noise and losses in the quantum channel, and the devices are perfect. The case with a practical quantum line and devices will be discussed in section IV. For the subsystem, the QSDC can be implemented with seven steps.

(1) All the users on the network agree that the server, Alice prepares an ordered N EPR pairs in the same quantum state $|\psi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C - |1\rangle_B|0\rangle_C)$ for the quantum communication in each round. Alice divides it into two sequences, S_B and S_C. The S_B is composed of all the B photons in the N ordered EPR pairs, and the S_C is composed of all the C photons.

(2) Alice sends the two sequences S_B and S_C to Bob and Carol, respectively.

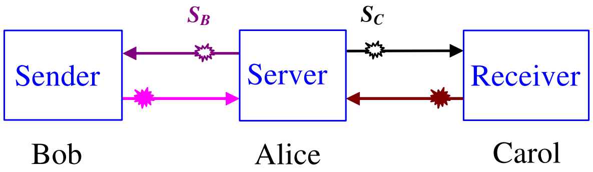

FIG. 1: The subsystem of the present QSDC network. There are two sequences of photons, S_B and S_C, which are transmitted to the sender Bob and the receiver Carol, respectively. The server, Alice provides the service for preparing and measuring the Bell states in the sequence of the EPR pairs. The legitimate users exploit the four local unitary operations to encode their message and complete the eavesdropping check with choosing one of the two measuring bases σ_z and σ_x randomly.

(3) After receiving the S_B and S_C sequences, Bob and Carol choose randomly a sufficiently large subset of the N EPR pairs as the samples for checking eavesdropping, and they measure each photon in each sample EPR pair with the measuring basis (MB) σ_z or σ_x chosen randomly. They complete the error rate analysis by comparing the outcomes in public, same as that in the Bennett-Brassard-Mermin 1992 (BBM92) QKD protocol [4]. If the error rate is zero, they continue to next step, otherwise they abandon their transmission and repeat the quantum communication from the beginning.

For preventing the eavesdropper, the dishonest server from eavesdropping by using Trojan horse attack with multi-photon signal [6] (For the attack with some invisible photons, the parties can exploit a suitable filter to allow just the photons with some a special frequency to be operated [6].), Bob and Carol can complete the eavesdropping check with two steps [41]. They can divide the samples into two parts. One is used to determine whether there are many photons in the sample signal. The other is used to determine whether the state of the quantum signal is disturbed. For the first part, the two parties, Bob and Carol can use a photon beam splitter to split the quantum signal, and measure them with two single-photon detectors. If there are many photons in the quantum signal received by the two parties, the two detectors will both be clicked with a large probability for each of the samples. In this way, the attack with Trojan horse can be found out. For the other samples, Bob and Carol measure them with two MBs σ_z and σ_x chosen randomly, same as that in Ref. [41].

For authenticating the outcomes published by Bob and Carol, they should share a certain amount of classical key in advance, or they have a special classical channel in which the information cannot be altered even though any one can eavesdrop it, same as QKD [6].

(4) Carol chooses randomly one of the four local unitary operations $\{U_0, U_1, U_2, U_3\}$ which represent the two bits of information 00, 11, 01 and 10 respectively, on each photon in the S_C sequence (except for the photons cho-

sen for eavesdropping check), and then she tells Bob the fact that she has operated her sequence S_C. She sends the S_C sequence to the server Alice. The operations done by Carol is denoted as U_C.

(5) Bob encodes his message on the photons in the S_B sequence with one of the four local unitary operations $\{U_i\}$ $(i = 0, 1, 2, 3)$, say U_B, according to the message M_B, and then she also sends the S_B sequence to the server Alice.

For analyzing the error rate of this transmission, Bob picks out k photons (the k sample photon pairs are composed of them and the correlated photons in the S_C sequence) randomly distributing in the S_B sequence and performs one of the four unitary operations randomly before he encodes the S_B sequence. The number k is not big as long as it can provide an analysis for the error rate.

(6) Alice performs Bell state measurements on the photon pairs and publishes the outcomes $U_A = U_B \otimes U_C$.

(7) Bob and Carol exploit the k photon pairs chosen as the sample pairs by Bob in advance to analyze the security of the whole quantum communication and estimate its error rate. In detail, Bob tells Carol her operations on the sample pairs and Carol compares them with the outcomes published by Alice. If the error rate is zero, Carol reads out the message M_B with $U_B = U_A \otimes U_C$. Otherwise, they discard the results.

In a QSDC network scheme, the most powerful eavesdropper may be the dishonest server Alice as she prepares the quantum signal and she can hide her eavesdropping with cheating besides other strategies. If it is secure for the untrustworthy server, the present QSDC network scheme is secure for any eavesdropper. So we only discuss the eavesdropping done by the server Alice below.

The operations U_C done by Carol are used to shield the effect of the code done by Bob. It is equivalent to encrypting Bob's message with an one-time pad cryptosystem. The random key is just the operations chosen randomly by Carol. In this way, the present QSDC network is secure if the transmission of the two sequences from the server Alice to the users Bob and Carol is secure as Alice's action on the last stage can only obtain the combined outcome $U_A = U_B \otimes U_C$ which will be published by the server and the cheat that Alice publishes a wrong information in both the first stage when the quantum signal is transmitted from Alice to the users and the last stage will be found out by Bob and Carol with the comparison of the outcomes of the k sample photon pairs. The transmission of the two sequences S_B and S_C from the server to the users is similar BBM92 QKD protocol [4]. The difference is just that the photons are transmitted in a quantum data block in the present scheme, but one by one in the latter. The BBM92 QKD protocol is proven secure in both an ideal condition [43] and a practical condition [44]. Hence, the present QSDC network scheme can be made to be secure. Moreover, as almost all the instances can be used to carry the message except for those for eavesdropping check, the intrinsic efficiency for qubits η_q in the present QSDC network scheme approaches the maximal value 1.

$$\eta_q \equiv \frac{q_u}{q_t}, \tag{11}$$

where q_u and q_t are the qubits useful and total qubits for the transmission. Each photon pair can carry two bits of message which is the maximal source capacity for a two-photon entangled state in quantum communication [6, 42]. The users (except for the server) are required to have the capability of single-photon measurements, which may make this network scheme convenient in application.

B. QSDC network with entanglement swapping

In a practical quantum channel, there are noise and loss which maybe affect the security of the network communication. The quantum channel, a sequence of EPR pairs in the same state $|\psi^-\rangle_{BC} = \frac{1}{\sqrt{2}}(|0\rangle_B|1\rangle_C - |1\rangle_B|0\rangle_C)$ can be set up securely with entanglement purification [32, 33]. But this case does not take place when the quantum states are encoded with the local operations. In this way, the users can accomplish the quantum communication with entanglement swapping [45]. In detail, the subsystem of the QSDC network can work as follows:

(1) The server Alice provides the service for Bob and Carol to securely share a sequence of EPR pairs in the same state $|\psi^-\rangle$, same as that in the bidirectional QSDC network scheme discussed above.

(2) After purifying the EPR pairs [32], Bob and Carol can obtain a short sequence of maximally entangled two-photon states. The two users divide them into some groups. There are two EPR pairs in each group, say $|\psi^-\rangle_{B_1C_1}$ and $|\psi^-\rangle_{B_2C_2}$. Bob encodes his message on the first EPR pair in each group with the operations U_i (i=0,1,2,3) and then performs a Bell-basis measurement on the photons B_1 and B_2. He announces his outcome in public.

(3) The receiver Carol takes a Bell-basis on his photons C_1 and C_2 to read out the message. That is,

$$\begin{aligned}
|\psi^-\rangle_{B_1C_1} \otimes |\psi^-\rangle_{B_2C_2} &= \frac{1}{2}(|\psi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2} \\
&\quad -|\psi^+\rangle_{B_1B_2}|\psi^+\rangle_{C_1C_2} - |\phi^-\rangle_{B_1B_2} \otimes |\phi^-\rangle_{C_1C_2} \\
&\quad +|\phi^+\rangle_{B_1B_2}|\phi^+\rangle_{C_1C_2}), \qquad (12) \\
|\psi^+\rangle_{B_1C_1} \otimes |\psi^-\rangle_{B_2C_2} &= \frac{1}{2}(|\psi^+\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2} \\
&\quad -|\psi^-\rangle_{B_1B_2}|\psi^+\rangle_{C_1C_2} + |\phi^+\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2} \\
&\quad -|\phi^-\rangle_{B_1B_2}|\phi^+\rangle_{C_1C_2}), \qquad (13) \\
|\phi^-\rangle_{B_1C_1} \otimes |\psi^-\rangle_{B_2C_2} &= \frac{1}{2}(|\phi^-\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2} \\
&\quad -|\phi^+\rangle_{B_1B_2}|\psi^+\rangle_{C_1C_2} - |\psi^-\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2} \\
&\quad +|\psi^+\rangle_{B_1B_2}|\phi^+\rangle_{C_1C_2}), \qquad (14) \\
|\phi^+\rangle_{B_1C_1} \otimes |\psi^-\rangle_{B_2C_2} &= \frac{1}{2}(|\phi^+\rangle_{B_1B_2}|\psi^-\rangle_{C_1C_2}
\end{aligned}$$

$$-|\phi^-\rangle_{B_1B_2}|\psi^+\rangle_{C_1C_2}+|\psi^+\rangle_{B_1B_2}|\phi^-\rangle_{C_1C_2}$$
$$-|\psi^-\rangle_{B_1B_2}|\phi^+\rangle_{C_1C_2}). \quad (15)$$

Carol can deduce Bob's operation according to the result of her Bell-state measurement and the information published by Bob easily.

In this QSDC network scheme, the sender Bob need not transmit the qubits to the server Alice after he encoded his message on them. That is, Bob and Carol do not give the chance for Alice to access the qubits again when the quantum channel (a sequence of EPR pairs shared) is confirmed to be secure. This principle will improve the security of the quantum communication in a noise condition as the qubits do not suffer from the noise and losses of the quantum line again. The effect of the noise in quantum line on the qubits which are transmitted between the server and the users can be eliminated with entanglement purification [32] and quantum privacy amplification [33]. Thus this network scheme can be made to be secure. On the other hand, the users should have the capability of taking a Bell-basis measurement on their qubits in this QSDC network scheme, which will increase the difficulty of its implementation in a practical application. Moreover, each EPR pair shared between the sender and the receiver can carry only one bit of information in theory, half of that in the bidirectional one.

IV. SECURITY ANALYSIS

In essence, the server Alice first provides the service for the users to share a sequence of EPR pairs in these two QSDC network schemes, and the two authorized users confirm the security of the quantum channel and then encode and decode the secret message after they purified their EPR pairs. With the analysis for the samples by using two MBs, σ_z and σ_x, the sender and the receiver can share securely a sequence of EPR pairs, similar to BBM92 QKD protocol [4]. The difference is just that all the qubits in BBM92 protocol are measured and the authorized users use classical privacy amplification to distill a private string. In these two QSDC network schemes, Bob and Carol can also use the entanglement purification [32] and quantum privacy amplification [33] to share a sequence of EPR pairs securely. In this way, their security can be the same one. As the security of the network schemes depend on completely that of the quantum channel, they are secure since the quantum channel can be made to be secure with entanglement purification [32, 33]. Surely, the users can use the technique of entanglement purity testing code [46] to save the entangled source largely for setting up their quantum channel.

We can also use the relation of the error rate and the correspondent maximal amount of information obtainable for the suspect server from a photon in each pair to demonstrate the security of the quantum channel set up following the ideas in Refs. [20, 47, 48, 49, 50, 51, 52, 53, 54, 55]. In fact, the effect of the eavesdropping on the two photons in an EPR pair with two unitary operations is equal to that on one photon with another unitary operation [56], i.e., $(U_{eB}\otimes U_{eC})|\psi^-\rangle_{BC}=(U_e\otimes I)|\psi^-\rangle_{BC}$. As Bob and Carol check eavesdropping with choosing the two MBs σ_z and σ_x randomly, same as the BBM92 QKD protocol [4], the eavesdropping done by Eve can be realized by a unitary operation, say, $\hat{E}$ on a larger Hilbert space. That is, Eve can perform the unitary transformation $\hat{E}$ on the photon B and the ancilla e [51, 53] whose state is initially in $|0\rangle$ [56].

$$\hat{E}|0\rangle_B|0\rangle = \sqrt{F}|0\rangle|e_{00}\rangle+\sqrt{D}|1\rangle|e_{01}\rangle, \quad (16)$$
$$\hat{E}|1\rangle_B|0\rangle = \sqrt{D}|0\rangle|e_{10}\rangle+\sqrt{F}|1\rangle|e_{11}\rangle \quad (17)$$

where F is the fidelity of the state of the photon B after the eavesdropping, D is the probability that Bob and Carol can detect the action of eavesdropper, and the unitary of the operation $\hat{E}$ requires the relations as follows

$$\langle e_{00}|e_{00}\rangle+\langle e_{01}|e_{01}\rangle=F+D=1, \quad (18)$$
$$\langle e_{10}|e_{10}\rangle+\langle e_{11}|e_{11}\rangle=D+F=1, \quad (19)$$
$$\langle e_{00}|e_{10}\rangle+\langle e_{01}|e_{11}\rangle=0. \quad (20)$$

With the unitary operation $\hat{E}$ done by Eve and the unitary operations U_i done by Bob with the probabilities P_i $(i=0,1,2,3)$, the final state of the photon B and the ancilla e is described as follows [50].

$$\varepsilon(\rho_B)=\sum_{i=0}^{3}P_i\varepsilon_{U_i}(\rho_B), \quad (21)$$

where P_i is the probability encoded with the operation U_i, $\rho_B=Tr_C(\rho_{BC})=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$, and ε_{U_i} is quantum operation describing the evolution of the initial state ρ_B, i.e.,

$$\varepsilon_{U_i}(\rho_B)=U_i\hat{E}\rho_B\otimes|e\rangle\langle e|\hat{E}^{+}U_i. \quad (22)$$

The accessible information extracted from the state $\varepsilon(\rho_B)$ is no more than the Holevo bound [20, 42, 50], i.e.,

$$I_C\leq S(\varepsilon(\rho_B))-\sum_{i=0}^{3}P_iS(\varepsilon_{U_i}(\rho_B))\equiv I_0, \quad (23)$$

where $S(\rho)$ is the von-Neumann entropy of the state ρ, i.e.,

$$S(\rho)=-Tr\{\rho log_2\rho\}=\sum_{i=0}^{3}-\lambda_i\log_2\lambda_i, \quad (24)$$

where λ_i are the roots of the characteristic polynomial $\det(\rho-\lambda I)$ [20]. As we use a mixed state to describe the photon B, Eve can steal the bit value or the phase of the operations done by Bob, same as Ref. [50]. In fact, the information that Eve can steal is no more than twice of I_0.

Certainly, Eve can eavesdrop the operation done by Bob U_B with two unitary operations and two ancilla systems, but it does not increase the information about the operation U_B and not decrease the probability D. Now, let us calculate the value of I_0 in the case that Carol chooses the four local unitary operations with the same probability $P_i = \frac{1}{4}$. Define an orthonormal base $\{|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle\}$ which spans the generic subspace of the Hilbert space $H_C \otimes H_e$ support of $\varepsilon(\hat{\rho}_C)$. With the Eqs. (16)-(24), we can obtain the relation between I_0 and the probability D as following.

$$I_0 \;=\; -Dlog_2D - (1-D)log_2(1-D). \qquad (25)$$

When $D = 0.25$, the information that Eve can obtain $I_E \leq 2I_0 = 1.62 < 2$. That is, Bob and Carol can set up the quantum channel securely with entanglement purification [32] and quantum privacy amplification [33], similar to QKD with a classical privacy amplification [42].

In a practical quantum channel, there are noise and losses which will threaten the security of quantum communication. The present QSDC network schemes are secure in a closely ideal condition, but it is also affected by the noise and the losses in a practical channel, same as the two-step QSDC protocol [13] and others [14, 15, 16, 20, 21, 22, 23, 24, 25]. The quantum states are transmitted in a quantum data in the present QSDC network scheme, which will ensure it to overcome the effect of the noise in the practical channel as the parties can use quantum privacy amplification technique [33] to improve the security of the quantum states transmitted. This advantage happens only in the QSDC schemes with quantum data block, such as Refs. [13, 14, 15]. In order to reduce the effect of the losses, another quantum technique, quantum teleportation [27] can be used to determine whether the receiver has obtained the photons sent by the server Alice in the process of the transmission for the S_C sequence, same as that in the two-step QSDC scheme [13]. That is, Carol should prepare another N EPR pairs and perform quantum teleportation on the photons in the S_C sequence with her EPR pairs. If the teleportation successes, she tells Bob to encode the correlated photon in the S_B sequence. On the other hand, the present network schemes can be also used to distribute a private key and the users need not exploit quantum teleportation to improve its security in a loss channel.

V. DISCUSSION AND SUMMARY

It is of interest to point out that the stream-QSDC schemes [20, 21, 22, 23, 24, 25] do not work for a network as they are only quasi-secure in a practical channel. It is difficult for the users to do the error correction and the privacy amplification in those QSDC schemes [20, 21, 22, 23, 24, 25]. In particular, the privacy amplification cannot be accomplished as the photon is transmitted one by one and the information transmitted is the deterministic message, not a random key. The QSDC schemes in Refs. [14, 15] cannot be used to complete the task of a QSDC network in a simple way as the server who prepares the quantum signal can steal almost all the information about the message without being found out in a noise channel. For example, in the QSDC network with the quantum one-time pad scheme [14], the server can intercept the photons encoded by Bob and read out the operations freely. Certainly, the two users can exploit some other technique to improve the security, but the classical information exchanged will increase largely, same as the QSDC schemes with quantum teleporation [17] and quantum swapping [18] which are close to QKD.

In summary, we have proposed two QSDC network schemes with EPR pairs. In the first one, the server prepares and measures the EPR pairs and the users exploit the four local unitary operations to encode their message, which makes the users on the network more convenient than others in a practical application. One can communicate any other one on the network securely as they can perform a quantum privacy amplification on the quantum states transmitted in a noise channel. Its intrinsic efficiency for qubits and source capacity are both high as almost all of the instances are useful and each EPR pair can carry two bits of information. In the second QSDC network scheme, the users exploit entanglement swapping to transmit the secret message, which will improve its security in a noise quantum line at the risk of lowering its source capacity and increasing the difficulty of the experimental implementation for the users. Also, the four requirements for a real secure point-to-point quantum direct communication scheme are discussed in detail and the present QSDC network schemes satisfy all the four requirements.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China under Grant Nos. 10447106, 10435020, 10254002, A0325401 and 10374010, and Beijing Education Committee under Grant No. XK100270454.

[1] W. K. Wootters and W. H. Zurek, Nature 299 (1982) 802.

[2] C. H. Bennett and G. Brassard, in: Proceedings of IEEE

International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, 1984 p175-179.

[3] A. K. Ekert, Phys. Rev. Lett. 67 (1991) 661.

[4] C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. 68 (1992) 557.

[5] C. H. Bennett, Phys. Rev. Lett. 68 (1992) 3121.

[6] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Rev. Mod. Phys. 74 (2002) 145.

[7] G. L. Long, X. S. Liu, Phys. Rev. A 65 (2002) 032302.

[8] F. G. Deng, G. L. Long, Phys. Rev. A 68 (2003) 042315.

[9] F. G. Deng, G. L. Long, Phys. Rev. A 70 (2004) 012311.

[10] L. -M. Duan M. D. Lukin, J. I. Cirac, P. Zoller, Nature 414 (2001) 413.

[11] H. K. Lo, H. F. Chau, M. Ardehali, J. Cryptology 18 (2005) 133.

[12] W. Y. Hwang, Phys. Rev. Lett. 91 (2003) 057901.

[13] F. G. Deng, G. L. Long, X. S. Liu, Phys. Rev. A 68 (2003) 042317.

[14] F. G. Deng, G. L. Long, Phys. Rev. A 69 (2004) 052319.

[15] C. Wang et al., Phys. Rev. A 71 (2005) 044305.

[16] C. Wang, F. G. Deng, G. L. Long, Opt. Commun. 253 (2005) 15.

[17] F. L. Yan, X. Zhang, Euro. Phys. J. B 41 (2004) 75.

[18] Z. X. Man, Z. J. Zhang, Y. Li , Chin. Phys. Lett. 22 (2005) 18.

[19] T. Gao, Z. Naturforsch. A 59 (2004) 597; T. Gao, F. L. Yan, Z. X. Wang, Nuovo Cimento B 119 (2004) 313; T. Gao, F. L. Yan, Z. X. Wang, Chin. Phys. 14 (2005) 893.

[20] K. Boström, T. Felbinger, Phys. Rev. Lett. 89 (2002) 187902.

[21] Q. Y. Cai, B. W. Li, Chin. Phys. Lett. 21 (2004) 601.

[22] B. A. Nguyen, Phys. Lett. A 328 (2004) 6.

[23] Z. X. Man , Z. J. Zhang, Y. Li, Chin. Phys. Lett. 22 (2005) 22.

[24] Q. Y. Cai, B. W. Li, Phys. Rev. A 69 (2004) 054301.

[25] M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94 (2005) 140501.

[26] A. Beige et al., Acta Phys. Pol. A 101 (2002) 357; J. Phys. A 35 (2002) L407.

[27] C. H. Bennett, S. J. Wiesner, Phys. Rev. Lett. 68 (1992) 3121.

[28] A. Wójcik, Phys. Rev. Lett. 90 (2003) 157901.

[29] Z. J. Zhang, Z. X. Man, Y. Li, Phys. Lett. A 333 (2004) 46; Phys. Lett. A 341 (2005) 385.

[30] Q. Y. Cai, Phys. Rev. Lett. 91 (2003) 109801.

[31] Z. J. Zhang, Z. X. Man, Y. Li, Int. J. Quant. Inform. 2 (2004) 521.

[32] C. H. Bennett,G. Brassard, S. Popescu, et al., Phys. Rev. Lett. 76 (1996) 722 ; C. H. Bennett, D. P. DiVincenzo, J. A. Smolin et al., Phys. Rev. A 54 (1996) 3824.

[33] D. Deutsch et al., Phys. Rev. Lett. 77 (1996) 2818.

[34] F. G. Deng, G. L. Long, e-print quant-ph/0408102.

[35] S. J. D. Phoenix , S. M. Barnett, P. D. Townsend, K. J. Blow, J. Mod. Opt. 42 (1995) 1155.

[36] P. D. Townsend, Nature 385 (1997) 47.

[37] E. Biham, B. Huttner, T. Mor, Phys. Rev. A 54 (1996) 2651.

[38] P. Xue, C. F. Li, G. C. Guo, Phys. Rev. A 65 (2002) 022317.

[39] F. G. Deng et al., Chin. Phys. Lett. 19 (2002) 893.

[40] C. Y. Li et al., Chin. Phys. Lett. 22 (2005) 1049; X. H. Li et al., Chin. Phys. Lett. 23 (2006) 1080.

[41] F. G. Deng, X. H. Li, H. Y. Zhou, Z. J. Zhang, Phys. Rev. A 72 (2005) 044302.

[42] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, Cambridge, UK, 2000).

[43] H. Inamori, L. Ralan, V. Vedral, J. Phys. A 34 (2001) 6913.

[44] E. Waks, A. Zeevi, Y. Yamamoto, Phys. Rev. A 65 (2002) 052310.

[45] M. Zukowski, A. Zeilinger, M. A. Horne and A. K. Ekert, Phys. Rev. Lett. 71 (1993) 4287; J. W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. 80 (1998) 3891; J. Lee, S. Lee, J. Kim and S. D. Oh, Phys. Rev. A 70 (2004) 032305.

[46] P. García-Fernández, E. Fernández-Martínez, E. Pérez and D. J. Santos, arXiv:quant-ph/0306068.

[47] A. Wójcik, Phys. Rev. Lett. **90**, 157901 (2003).

[48] I. P. Degiovanni, I. R. Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, Phys. Rev. A 69 (2004) 032310.

[49] A. Wójcik, Phys. Rev. A 71 (2005) 016301.

[50] I. P. Degiovanni, I. R. Berchera, S. Castelletto, M. L. Rastello, F. A. Bovino, A. M. Colla, and G. Castagnoli, Phys. Rev. A 71 (2005) 016302.

[51] M. Lucamarini and S. Mancini, Phys. Rev. Lett. 94 (2005) 140501.

[52] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, and A. Peres, Phys. Rev. A 56 (1997) 1163.

[53] N. Gisin and R. B. Griffiths, Phys. Rev. A 60 (1999) 2764.

[54] A. Sen(De), U. Sen, and M. Żukowski, Phys. Rev. A 68 (2003) 032309.

[55] V. Scarani and N. Gisin, Phys. Rev. Lett. 87 (2001) 117901.

[56] J. Preskill, http://www.theory.caltech.edu∼preskill/ph229.